REVISTA DE CIÊNCIA ELEMENTAR

Congruências

João Nuno Tavares*, Ângela Geraldo[ı]
* Faculdade de Ciências da Universidade do Porto
[ı] CMUP/ Universidade do Porto

CITAÇÃO
Tavares, J. N., Geraldo, A.(2017) Congruências, *Rev. Ciência Elem.*, V5(01):070. doi.org/10.24927/rce2017.070

EDITOR
José Ferreira Gomes
Universidade do Porto

RECEBIDO EM
12 de janeiro de 2013

ACEITE EM
17 de julho de 2013

PUBLICADO EM
31 de março de 2017

rce.casadasciencias.org

Seja m um inteiro positivo. Dois inteiros a,b$\in \mathbb{Z}$ dizem-se congruentes módulo m se a diferença a−b é um múltiplo inteiro de m:

$$a-b=km, \text{ para algum inteiro } k\in\mathbb{Z}$$

Nesse caso escreve-se

$$a \equiv b \pmod m$$

Por exemplo
$19 \equiv 5 \pmod 7$, porque 19−5=14 é múltiplo inteiro de 7.
$31 \equiv -2 \pmod 3$, porque 31−(−2)=33 é múltiplo inteiro de 11.
$12 \equiv 39 \pmod 9$, porque 12−39=−27 é múltiplo inteiro de 9.
$16 \equiv -9 \pmod 5$, porque 16−(−9)=25 é múltiplo inteiro de 5.

Mas, por exemplo, 3 não é congruente com 11 (mod 7), porque 3−11=−8 não é múltiplo inteiro de 7.

Propriedades
A propriedade seguinte será usada na dedução dos chamados critérios de divisibilidade.

Teorema
Dois inteiros a,b$\in \mathbb{Z}$ são congruentes módulo m se e só se produzem o mesmo resto quando divididos por m.

Demonstração
Suponhamos que $a \equiv b \pmod m$, e que a=qm+r, com q,r$\in \mathbb{Z}$ e $0\leq r<m$. Então a−b=km,k$\in \mathbb{Z}$. Substituindo a=qm+r, vem que b=a−km=qm+r−km=(q−k)m+r, com q−k$\in \mathbb{Z}$ e $0\leq r<m$, o que significa que o resto da divisão de b por m também é r.
Reciprocamente, se a=qm+r e b=q´m+r com q,q´,r$\in \mathbb{Z}$, 0 r<m, então b−a=q´m+r−qm−r=(q´−q)m, o que significa que $a\equiv b \pmod m$, CQD.

Mais propriedades
· Sejam d, n$\in \mathbb{N}$ e a, b$\in \mathbb{Z}$. Temos que:

(i) $a \equiv a \pmod n$;
(ii) se $a \equiv b \pmod n$, então $b \equiv a \pmod n$;

(iii) se a ≡ b(mod n) e b ≡ c(mod n), então a ≡ c(mod n);
(iv) se a ≡ b(mod n) e d|n então a ≡ b(mod d).

Demonstração
(ii) Se a ≡ b(mod n) então a−b=kn ⇔ a=b+kn com k∈ ℤ. Ora então b−a=b−(b+kn)=−kn, ou seja, b−a é um mútiplo inteiro de n e portanto b ≡ a(mod n).
(iii) Se a ≡ b(mod n) então a−b=kn ⇔ a=b+kn com k∈ ℤ. Se b ≡ c(mod n) então b−c=t-nÐc=b−tn com t∈ ℤ. Ora, a−c=(b+kn)−(b−tn)=kn+tn=(k+t)n, ou seja, a−c é um múltiplo inteiro de n, isto é, a ≡ c(mod n).
(iv) Se a ≡ b(mod n) então a−b=kn com k∈ ℤ. Ora, se d|n podemos escrever n=td com t ∈ ℤ. Temos então que a−b=kn=k(td)=(kt)d, como kt é um número inteiro, concluímos que a−b é um múltiplo inteiro de d, ou seja, a ≡ b(mod d).

- Seja n∈ ℕ e sejam a, b, c e d∈ ℤ. Temos que:
  (v) se a ≡ b(mod n) e c ≡ d(mod n), então a+c ≡ b+d(mod n);
  (vi) se a ≡ b(mod n) e c ≡ d(mod n), então ac ≡ bd(mod n).

Demonstração
(v) Sejam r e s inteiros tais que, a−b=rn e c−d=sn. Então, (a+c)−(b+d)=(a−b)+(c−d)=rn+s-n=(r+s)n, isto é, (a+c)−(b+d) é um múltiplo inteiro de n e portanto a+cÐb+d(mod n).
(vi) Observemos que ac−bd=ac−bc+bc−bd=(a−b)c+(c−d)b=rnc+snb=(rc+sb)n, ou seja, ac−bd é um múltiplo inteiro de n e então acÐbd(mod n).